A Strategy for the Development of Secure Telemedicine Applications

Ravi S. Raman, Ramana Reddy, V. Jagannathan,
Sumitra Reddy, K. Joseph Cleetus and K. Srinivas
Concurrent Engineering Research Center
West Virginia University
Morgantown WV 26506-6506

Healthcare applications based on computer-supported collaboration technologies have the potential to improve the quality of care delivered to patients. Such applications can help overcome barriers to quality healthcare in the small, scattered populations of rural areas enabling telemedicine to be a part of the practice of medicine. However the growing concern about the potential for abuse through disclosure of personal health information to unauthorized parties has restricted the deployment and adoption of these potentially valuable tools. The authors, who built ARTEMIS -- an Intranet healthcare collaboration facility, now describe their approach to develop secure telemedicine applications for rural healthcare practitioners.

INTRODUCTION

The growth of the World Wide Web and other Internet-based applications as well as the increasing use of computers in the businesses and homes of healthcare providers for electronic mail and to access computer-based patient records have fostered the hopes of collaboration among healthcare providers. However, there are legitimate concerns about the security of electronic medical information – by unauthorized access on-site or from afar; by interception and modification during transmission over a local area network or the Internet; as well as the opportunities through aggregation for the misuse of personally identifiable healthcare records. Privacy and confidentiality issues are of great interest to the public at large and have been the focus of numerous organizations and books [1,2,3] and techniques to support privacy and confidentiality are currently popular topics at many conferences.

The report on the privacy and security of electronic healthcare information by the National Research Council's Computer Science and Telecommunications Board [4] identifies a number of risks:

- disclosure of sensitive information by privileged healthcare providers;
- unauthorized access to sensitive healthcare information;
- ability of database pattern matching to identify individuals from collective data; and
- undetected and unauthorized alterations of electronic health information.

A combination of administrative procedures and technical means along with legislative and regulatory measures may be employed to address these risks.

COLLABORATION TECHNOLOGY

Since 1993 the Concurrent Engineering Research Center (CERC) at West Virginia University has been developing computer-supported collaboration technologies and applications for clinical healthcare providers. The system, called ARTEMIS [5], funded jointly by the US Defense Advanced Research Projects Agency (DARPA) and the US National Library of Medicine (NLM), was among the first to enable healthcare providers to access distributed clinical patient records utilizing the World Wide Web. Developed in partnership with healthcare practitioners, CERC's ARTEMIS system attracted the attention of the national media in the United States by illustrating the use of the World-Wide Web as a means to access electronic medical records. ARTEMIS is currently undergoing field trials [6,7] and evaluations [8] at a set of rural healthcare facilities. A companion paper at this conference discusses our experience in developing and deploying ARTEMIS in rural healthcare facilities [9].

1091—8280/97/$5.00

Administrative measures

Employee screening
Training
Chain of responsibility
Disciplinary measures

Patient disclosure and review
Fair-use policy

Procedural measures

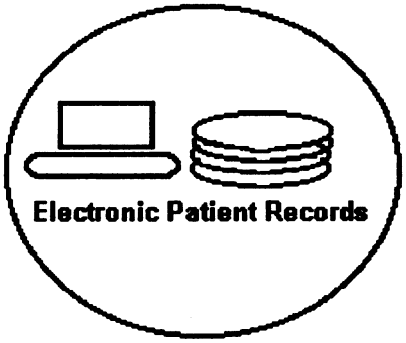
Password policy
Backup and restoration
Disaster recovery
Secure and remote storage of archives

Virus scans
Access log review
Intrusion event handling

Technical measures

Identification
Encryption
Access control
Audit trails

Non-repudiation
Firewalls
Dial-back modems
Screen locks



Implementation of Security Policies for Electronic Patient Records

The focus of the ARTEMIS project had been the development of technologies to support Web-based access to electronic medical records. Many innovative developments were developed such as dynamic creation of HTML pages using medical record templates, CORBA/HTTP integration [10], a customized Web browser that supported viewing of multi-document electronic patient records along with support for dictation of encounter notes and a Web-based document signoff facility. The system utilized password-based user access control measures and session time-out mechanisms as well as firewall-based perimeter protection.

The security technology that is now widely available has matured rapidly in the past few years. Of particular note are the public key cryptography and digital signature technologies and the growing number of systems that employ them. Web browsers and Web servers utilize X.509 v3 certificates to enable user and site authentication. Mail programs employ message digest and encryption facilities for secure e-mail. There appears to be a gradual, but grudging, acceptance by users of the need for such facilities to ensure secure transactions.

Legislative measures to protect personal healthcare information have been enacted in the US (HIPA PL104-191) and more have been proposed in the 105th Congress (e.g., HR52). These legislative measures place a significant responsibility on healthcare organizations and providers to adequately protect the healthcare information in their charge.

Healthcare organizations can employ a number of computer system security measures to protect their information system assets. For instance:

1. Enterprise perimeters can be protected from physical and electronic intrusion. Data records can be housed separate from the organization, and in fire and moisture proof facilities.
2. Firewalls, dial-back modems, virus checks and regular monitoring of access logs provide measures against electronic intrusion.
3. Security at all point-of-service computers and terminals can be ensured using user authentication measures. When these terminals

are briefly unattended, automatic screen locks and screen modifiers can prevent improper access or inadvertent disclosure of healthcare information. Role-based access techniques can be used to ensure that information is provided on a need-to-know basis.

4. Workstation security can be increased using smart card/encryption card systems. These are tamper-proof, hardware-based systems which authenticate users through encryption and digital signature operations performed entirely on the token.
5. Secure transactions in distributed systems can be achieved by addressing the security issues of the communication pipe and processes at its end points, namely clients and servers. Communication pipe security can be addressed by link encryption to ensure the privacy and integrity of healthcare information while it is in transit. Client end security can be achieved by authentication measures using tokens like smart cards to protect key information from hard/floppy disk or key-stroke disclosures. While server end points can be secured using firewall and database security mechanisms.
6. Electronic healthcare records can be protected by applications and servers incorporating and abiding by authenticated, authorized and audited access control facilities.

In addition, healthcare organizations can employ administrative procedures, such as fair-use policies, employee training and patient disclosure and review procedures, to ensure the integrity and confidentiality of their patients' electronic health information.

However, implementation of these technologies and procedures vary among healthcare organizations due to a number of reasons including budget, organizational expertise, technically obsolete legacy information systems, size and location of organization, and perception of invulnerability.

SECURE TELEMEDICINE

CERC is now engaged in a new three year contract under the sponsorship of the U.S. National Library of Medicine, to develop and deploy applications for secure collaborative telemedicine in rural areas of the United States and to evaluate its impact on the delivery of healthcare.

A set of three telemedicine scenarios have been identified that enable healthcare providers to collaborate in the treatment of patients. These scenarios illustrate the utility of collaborative telemedicine technologies to improve the delivery of healthcare at rural hospitals, clinics, and homecare sites:

1. Secure telemedicine for intensive care providers enabling remote access of Intensive Care Unit electronic patient data.

2. Secure telemedicine for mid-level providers (such as physician assistants and nurse practitioners) providing computer-aided diagnosis and collaboration with remote supervising physicians.

3. Secure telemedicine for homecare patients through patient counseling information resources and support for near-time monitoring of patients with chronic ailments.

These telemedicine applications could be realized with current technology using vendor proprietary solutions. However, a collaborative telemedicine system must be integrated with the patient record service services and related applications at each of the point of care facilities in which it is operational. Proprietary healthcare information systems have made such integration expensive and limited in scope and scale. Open standards based interfaces to healthcare systems would enable healthcare organizations to more easily and less expensively integrate these systems. The challenges being addressed by this research effort are to enable these services while ensuring security of information, and ensuring their evolution with technology without being locked in to expensive, sole source systems.

We are developing a Secure Collaborative Telemedicine Architecture (SCTA) using an open systems approach, utilizing vendor-supported, standards-compliant components and technologies. To ensure scalability and broad usage, we are using CORBA (Common Object Request Broker Architecture) which is supported by over 600 vendors world-wide. Object Request Brokers with intrinsic support for secure transactions, such as Suite Software and Iona Technologies are now emerging. We believe that CORBA, in conjunction with allied encryption technologies offers the best-cost solution for implementing secure distributed

systems. In addition we are employing vendor-supplied bridge facilities to accommodate other standards, such as Microsoft's Distributed Component Object Model (DCOM) for integration and site-specific customization with essential applications and systems on client and server systems.

An infrastructure to support secure collaborative telemedicine transactions should provide as its core capabilities:

- a security infrastructure that supports authentication and the secure transmission of private and confidential patient information;
- transparent and easy access to distributed patient information;
- a secure workflow in the context of patient treatment; and
- a secure consultation service in the context of patient information and a patient treatment plan.

In our view, support for the above services constitutes the core backplane for telemedicine applications. Other services can be plugged into this backplane to provide a variety of custom support features to a variety of specific providers including:

- real-time or near real-time access to information gathered by instruments monitoring a patient;
- seamless access to clinical decision support systems and on-line knowledge repositories such as MedLine.

The authentication services of the SCTA will support measures to restrict access to authenticated and authorized personnel. We are adopting industry-standard, multi-platform cryptography solutions to develop a secure, open, collaborative technology infrastructure which supports the distributed components of our telemedicine applications.

The SCTA services will be incorporated into our telemedicine applications and customized to meet the organizational needs of the healthcare facility and its telemedicine users. For secure operation it must work in concert with its technological and administrative procedures and be in compliance with the security policies of the healthcare network.

Periodic inspections of security policies and procedures will determine the efficacy of these measures and enable corrective action to be taken.

Secure middleware components must utilize authentication services that support measures to restrict access to authenticated and authorized personnel. Such authentication services, based on industry-standard cryptography solutions, can provide the infrastructure to support distributed component healthcare applications.

A smart card resembles a credit card in size and shape, and stores information and instructions on an integrated microprocessor chip located on the card. Smart cards can store around 8 Kbytes of information and, in some cards, perform on-chip encryption. Through the use of X.509v3 digital certificates and via a Certificate Server and a Directory Server, a healthcare organization can authenticate its healthcare providers and enable their credentials to be verified on-demand by crypto-aware applications and servers. PIN protected smart cards can store an individual's private keys and certificates enabling authenticated use at any point of care system as well as digital signature operations.

New crypto-aware applications can incorporate these security measures to ensure the privacy and security of healthcare information. Legacy systems can be "wrapped" to make them accessible by these new applications.

We are planning on using PIN protected smart cards in our telemedicine applications for the identification and authentication of providers, and the storage of limited patient medical information. Using Schlumberger's Multiflex smart cards we have developed experimental prototypes of healthcare professional and patient cards. Based on the EU/G7 healthcard format, the patient cards contain patient demographics, insurance information as well as clinical information for clinical emergencies. Role-based access measures distinguish between the needs of administrators, physicians and nurses.

Remote viewing of patient vital signs information is an important element in all three telemedicine applications where healthcare providers are separated from the patient. We have developed Java-based client applications for the remote viewing of vital signs information as well as Java-based CORBA vital signs servers.

We have also developed experimental prototypes of CORBA filters and transformers to ensure secure communications between client applications, and server and middleware services. An experimental

prototype of the ARTEMIS system was migrated to S-HTTP, albeit without the use of CORBA security measures.

We will be deploying initial prototypes of our telemedicine application in selected pilot sites by the end of 1997. Periodic releases of applications with additional functionality are planned at three month intervals through 1998.

CONCLUSIONS

Cryptography technologies incorporated into healthcare collaboration applications hold out the promise of improving the quality and access to care. In combination with other data security techniques and organizational procedures, they could help improve the privacy and integrity of healthcare information. As a result, patients everywhere, not just in the small, scattered populations of rural areas, could overcome the traditional barriers to quality healthcare without compromising the privacy of their medical information. Recently, three of RSA Laboratories' challenges for deciphering encrypted messages have been successfully decoded through the use of a very large number of computers. Such exposes will, we feel, spur the use of better cryptographic solutions than those currently permitted by the US government. Healthcare and business transactions will both benefit as a consequence.

Acknowledgments

This work has been sponsored by the U.S. National Library of Medicine under Contract No. N01-LM-6-3549. Other CERC employees who have contributed to this research effort include Rahul Singhal, Srivatsan Kannan, William Hunt, Vic Baker and Cristi Goina.

References

1. Rothfeder, J. Privacy for Sale: How Computerization Had Made Everyone's Life an Open Secret. New York: Simon; 1992.

2. Donaldson MS, and Lohr KN, editors. Health Data in the Information Age: Use, Disclosure, and Privacy. Washington, DC: National Academy Press; 1994.

3. Alderman E, and Kennedy C. The Right to Privacy. New York: Knopf; 1995.

4. Computer Science and Telecommunications Board, National Research Council. For The Record: Protecting Electronic Health Information. Washington, DC: National Academy Press; 1997.

5. Jagannathan V, Reddy R, Srinivas K, et al. An Overview of the CERC ARTEMIS Project. Proceedings of the 19th Annual Symposium on Computer Applications in Medical Care (SCAMC); 1995. p. 12-16.

6. Reddy S, Shank R, Jagannathan V, Merkin B. A Virtual Enterprise for Rural Health Care Through Advanced Communication and Information Technologies. Proceedings of the Annual Review of Communications. International Engineering Consortium; 1996. p. 631-36.

7. Reddy S, and Jagannathan V. Applications of Collaborative Technology: From Engineering to Health Care. Proceedings of the International Workshop on CSCW in Design - Session 3: Applications; 1996. p. 445-50.

8. Galfalvy HC, Reddy S, and Merkin B. Evaluation of a Community Care Network (CCN) System in a Rural Health Care Setting. Proceedings of the 19th Annual Symposium on Computer Applications in Medical Care (SCAMC); 1995. p. 698-702.

9. Jagannathan, V, Almasi G. Integrating the WWW and CORBA-Based Environments. First Class 1996; 6:1 13-16.

10. Reddy S, Niewiadomska-Bugaj M, Reddy YV et al. Experiences with ARTEMIS - An Internet-Based Telemedicine System. Proceedings of the 1997 AMIA Annual Fall Symposium. In press 1997.